Section III:

AMENDMENT UNDER 37 CFR §1.121 to the DRAWINGS

No amendments or changes to the Drawings are proposed.

Section IV:

AMENDMENT UNDER 37 CFR §1.121

REMARKS

Objections to the Claims

In the Office Action, several objections to claims were made:

> *Examiner in the Office Action:*
> Claims 2, 9 and 16 are objected to for lack of antecedent basis:
> Claim 2 recites "the next unused pad" in line 4.
> Claim 9 recites "the next unused pad" in line 5.
> Claim 16 recites "the next unused pad" in line 5.

With respect to "the next unused pad" recited in Claims 2, 9 and 16, by "pad", Applicant means a "pad value" recited in Claim 1 being marked as "unused" (see first, third and fifth elements). A one-time pad cryptological table contains a sequence of pad values to be used only once, and then marked as "previously used". When a pad value in a OTP table is marked "used", the pad value immediately following it is the "next unused" pad value, such as by using a "sequence index" as Applicant has disclosed (emphasis added by Applicant):

> *Applicant's Disclosure:*
> [0045] OTP cryptology approaches require that both ends of a sender - receiver relationship share an encryption key that is the result of a **randomly generated key sequence**. To decrypt a received message, the receiver must possess or derive a matching OTP to decipher the information in the message.
> . . .
> [0047] The table (30) in FIG. 3 depicts an example of **OTP values and sequence**, a copy of which would be stored or available to both the client and the service provider (or security server for the service provider). . . .
> [0048] The **Sequence index** (33) allows the device to easily manage which set of UID (32), ESN (31) and Session ID (34) are currently being used. Additionally, the **Used parameter (35) marks which entries in the table have been used already**, and which entries are still available for use, in order to avoid reuse of a previously used code set.

> . . .
>
> [0051] During legitimate, bona fide use or consumption of service according to our invention, the client device, such as a cell phone, initiates (42) a service session, such as a telephone call, during which the **next unused OTP entry is provided in the service request**. The enhanced service provider (16') proceeds with a verification process (43) to compare the OTP provided by the client with its own OTP entries (49) associated with the appropriate customer or device, and determines if this is the **next expected unused entry** in its own copy of the OTP table (49). As this is the legitimate, authentic device, the two tables (49) stored by the client (13') and the service provider (16') should be in synchronization with each other at this point.

To remove any possible confusion regarding the language of Claims 2, 5, and 16 applicant has amended them to recite "~~the~~ a next unused pad value" rather than "the next unused pad". Withdrawal of the objections is respectfully requested.

Rejections under 35 U.S.C. §103(a)

In the Office Action, Claims 1-5, 7-12, 14-19 and 21 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shefi (Patent No.: US 6,445794 Bl) in view of Müller (Klaus Müller, Siemens AG, "Intermediate report on UMTS security mechanisms: USECA"; April 1999, p. 1 - 73), hereinafter referred to as Shefi and Müller, respectively.

Rejections of Independent Claims 1, 8 and 15

It was reasoned in rejection of the independent claims that Shefi discloses the claimed steps, elements and limitations regarding providing the client and server with matching OTP value tables. Applicant respectfully disagrees. Shefi is directed towards methods to *generate* OTP tables in two or more locations simultaneously. Please note several references in Shefi's disclosure regarding using one random number added to a pseudo-random number to create a next random number, etc. Shefi's method could be used to *create* the OTP table which is then *provided* to the Applicant's client and server components, for example. By reciting "providing", Applicant is claiming only that the OTP tables have already been created by any known OTP table creation method, such as that of Shefi's method.

With respect to the shortcomings of Shefi's teachings as set forth in the Office Action, Applicant agrees that Shefi fails to teach the remainder of the claim steps, elements, and limitations. However, Applicant respectfully disagrees that Müller discloses the rest of the steps, elements, and limitations, as was addressed in Applicant's disclosure:

> *Applicant's Disclosure:*
> [0025] A more advanced approach to security has been discussed by the USECA (UMTS SECurity Architecture) group in its paper entitled "USECA D06 Intermediate report on UMTS security mechanisms", wherein UMTS abbreviates "Universal Mobile Telecommunications System". . . .
> [0026] However, certain questions remain unresolved, and potential vulnerabilities exist even with this improved approach, including:
>
> (a) their "count", which is a value shared between a phone attempting to access network services and an authorization or security server, can be rolled over, apparently to a maximum of 28, using just a 6-bit value;
>
> (b) their "count" value is automatically updated on both client and server, apparently without using a separate two-phase commit process to ensure that the "count" value stays synchronized between the two;
>
> (c) their "count" continues until there is a conflict, but a conflict is not initiated until a user dials in, following which the detected conflict apparently revokes the handset's service entirely, but it is not clear whether or not this provides a means to initiate a denial of service attack;
>
> (d) their "count" characteristics is dependent on local Home Environment Service Network ("HE/SN") service agreements;
>
> (e) their "count" value is not persistent on the client device, so there is no capability for non-repudiation;
>
> (f) their "count" is communicated from the network server to the client device as clear data wrapped in encryption, such that if the encryption is compromised, the "count" is compromised, thereby allowing both the original and the clone to be intercepted; and

(g) it appears that multiple clones can be programmed to recapture the correct count.

Please note that Müller's Call History Count ("COUNT") is one of several values shared between the mobile station ("MS") and the Home Environment Authentication Center ("HE/Auc") (emphasis added by Applicant):

Müller on Page 25:

• Call history count update

Procedure to support the update of the **call history counter *COUNT*** of a MS in a visited system. The aim of the call history counter is to simplify clone detection.

Müller on Page 26:

The authentication result AUTHR is computed by the MS from the random number RG (and the electronical serial number ESN of the handset and the first part of the mobile identification number MIN1) using CAVE under control of the temporary user specific authentication key SSDA. The **MS then sends** MIN, ESN, AUTHR, **its Call History Counter *COUNT***, and RCG (the first 8 significant bits of RG) **to the SN, which forwards these parameters to the HE/AuC**,replacing RCG by RG.

The HE/AuC verifies MIN and ESN. It then calculates the expected authentication response XAUTHR analogous to the calculation in the MS, and checks if AUTHR and XAUTHR match. The HE/AuC then **verifies that the COUNT** received from the MS is consistent with the value currently stored at the HE/AuC.

If this is not the case the HE/AuC responds with "Deny Access". Otherwise the response includes SSD and if needed directives to update the SSD or the call history counter COUNT of the MS according to the SN-HE agreed local administrative practices. The SSD Update procedure is described below. **The COUNT Update procedure is not described in this document**.

Müller's system is highly dependent on the call history COUNT value, disclosing its need and use throughout the paper, and showing its requirement in the protocol diagrams.

Applicant's invention, however, is operable without the security risks posed by the sharing, use and dependency on a call history count value, solving the problems described and discovered by Applicant (see paragraphs [0025] - [0026]). Applicant has amended the independent claims to recite this advantageous aspect of the invention, which is not disclosed or alluded to by Müller. Applicant respectfully requests allowance of Claims 1, 8 and 15 for these reasons.

Removing COUNT from Protocol or Process Not An Obvious Modification. To remove use and dependency of Müller's COUNT variable from their processes would be unobvious because there would be no motivation to change a fundamental principle of operation of their processes.

> *MPEP §2143.01 states:*
> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious.

Applicant respectfully requests allowance of Claims 1, 8 and 15 for these reasons.

Müller is Not Enabling Regarding Call History COUNT Updating. Müller clearly states that "[t]he COUNT Update procedure is not described in this document" (pg. 26, last sentence of last paragraph). Therefore, even if Müller's COUNT is held to teach some portion of Applicant's claims, it is not enabled by Müller's disclosure, and thus is disqualified as prior art. Applicant respectfully requests allowance of Claims 1, 8 and 15 for these reasons.

Ordinary Level of Skill in the Art Not Properly Established. In the Office Action, it was stated:

> *Examiner in the Office Action:*
> . . . it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

However, Applicant was not notified what the level of ordinary skill in the art was determined to be at the time of Applicant's invention. According to the Court in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), it is critical to determining obviousness under 35 U.S.C. §103 to ascertain the level of ordinary skill in the art, whereas this is pivotal in the language and standard set forth in the law at §103.

In the Office Action, the Applicant has not been notified what was considered to be the level of ordinary skill in the art. It is not clear if any of the criteria to be considered in determining the level of ordinary skill in the art under the third factual inquiry of *Graham v. John Deere,* as set forth in *Environmental Designs, Ltd. v. Union Oil,* 713 F.2d 693, 696, 218 USPQ 865, 868 (Fed. Cir. 1983) and in *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 449-450, 230 USPQ 416, 420 (Fed. Cir. 1986) such as (1) the educational level of the inventor, (2) the tpe of problems encountered in the art, (3) the prior art solutions to those problems, (4) the rapidity with which innovations are made by others, not including the inventor, (5) the sophistication of the technology, and (6) the educational level of active workers in the field not including the inventor, were considered, and if so, how.

Applicant respectfully submits that an obviousness rejection without such a determination would be improper. Applicant requests allowance of Claims 1, 8, and 15, or alternatively, if the rejection under 35 USC §103 is maintained, that the rejection not be made final until the Applicant has had an opportunity to respond to any determination of skill level per the Court's instructions in *Graham v. John Deere.*

Proposed Combination under 35 U.S.C. §103(a) Requires Unreasonable Leap in Concepts. Applicant respectfully submits that based on the foregoing facts, it would not have been a reasonable progression in logic or conception for an ordinarily skilled person in the art to modify and combine the cited references as proposed. For this reason, Applicant respectfully requests allowance of Claims 1, 8, and 15.

Rejections of Dependent Claims 2 -5, 7, 9 - 12, 14, 16 - 19, and 21

In the Office Action, Claims 2 -5, 7, 9 - 12, 14, 16 - 19, and 21 were rejected reasoning that the steps, elements, or limitations recited in addition to those presented in Claims 1, 8 and 15 from which they depend are taught by Müller.

Applicant respectfully disagrees for at least the reasons set forth in the foregoing paragraphs because Shefi in view of Müller fails to teach or suggest all of the claimed steps, elements and limitations of Claims 1, 8, and 15.

Applicant also respectfully submits that the rejection under 35 USC §103(a) is improper because no determination of an ordinary level of skill in the art at the time of Applicant's invention as instructed by the Court in *Graham v. John Deere* has been indicated and used in the analysis of what would have been obvious to do at the time of the invention.

For these reasons, Applicant requests allowance of Claims 2 -5, 7, 9 - 12, 14, 16 - 19, and 21.

Rejections of Claims 4, 11, and 18

With respect to the rejections of Claims 4, 11, and 18, Applicant respectfully disagrees that Müller teaches these claimed aspects of Applicant's invention.

Challenging a User Is Not The Same as Challenging the Device. By "challenge *the user*", Applicant means requiring the human user of the client device to input information which is known to the user, but not known or stored by the client device. For example, the user might input his or her password, or his or her account number. The claim language specifies that the user is challenged, not the device. Otherwise, the term "input" would not be necessary in the claim (e.g. the challenge response value would be previously stored or calculated at the time of the challenge).

The language of Müller's disclosure is a bit confusing because it refers to the human user of a client device and the client device itself collectively as "user". But, upon close consideration of Müller's disclosure and the protocol diagrams, their challenge response is "computed" using the client device's serial number, a portion of device's identification number, in combination with a random value RAND. These are not values which a human user would know, and unlikely would be unable to perform the computations described due to the length and format of these numbers (e.g. human users do not perform manipulations well on alpha-numeric base-16 serial numbers). Therefore, Applicant submits that Müller challenges the device, not user.

Müller's system relies upon stored and computed values by the client device, and thus if a client device is completely cloned, it would also have the same stored values and computation capabilities. Thus, Müller's challenge to the client device (not to the user) may be ineffective in detecting fully cloned devices.

Müller's RAND Value Is Not an OTP Pad Value. Also, please note that the random value RAND used in their protocols is not a OTP pad value as claimed. Applicant has claimed the client device sends the OTP pad value to the authentication server, but Müller has disclosed the reverse exchange direction – the RAND value is sent from the authentication server HE/AuC to the client device. Note especially the random number generator in the HE/Auc (upper right corner of Fig. 0-1 pg. 17 and center of Fig. 0-2 pg. 19), and direction of transmission of RAND from authentication center AuC to the client (not client to AuC) in centers of Figs. 0-1, 0-2, and 0-3.

For these additional reasons, Applicant respectfully requests allowance of Claims 4, 11, and 18.

Rejections of Claims 7, 14, and 21

With regard to the rejections of Claims 7, 14, and 21, it was reasoned that Müller discloses requirement of a second step to acknowledge that a OTP pad value has been previously used in Müller's teaching regarding the challenge of the user. Applicant respectfully disagrees.

Challenging the user is performed responsive to the OTP pad value *not matching* an expected next unused value, but the claimed "second step" is a confirmation step performed responsive to an exchanged OTP value *successfully matching* the next unused value in the OTP pad table.

For these additional reasons, Applicant respectfully requests allowance of Claims 7, 14, and 21.

Rejections of Dependent Claims 6, 13, and 20

In the Office Action, Claims 6, 13, and 20 were rejected reasoning that the steps, elements, or limitations recited in addition to those presented in Claims 1, 8 and 15 from which they depend are taught by Douceur.

Applicant respectfully disagrees for at least the reasons set forth in the foregoing paragraphs because Shefi in view of Müller in further view of Douceur fails to teach or suggest all of the claimed steps, elements and limitations of Claims 1, 8, and 15. Applicant also respectfully submits that the rejections under 35 USC §103(a) are improper because no determination of an ordinary level of skill in the art at the time of Applicant's invention as instructed by the Court in *Graham v. John Deere* has been indicated and used in the analysis of what would have been obvious to do at the time of the invention.

For these reasons, Applicant requests allowance of Claims 6, 13, and 21.

Summary

It is believed that each ground of objection and rejection have been addressed through amendment and/or reply remarks. Should the Examiner find that one or more grounds have not been addressed, Applicant respectfully requests to be notified of any deficiency.

Applicant has pointed out certain examples of support for the foregoing remarks found in the Applicant's disclosure, but the support is not limited to these example passages. The claims are part of the specification, and thus all of the claim terms should be given their scope and meanings as set forth in the entire disclosure:

> *35 U.S.C. 112:*
>
> . . .
>
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
>
> . . .

Federal Circuit regarding Interpretation of Claim Terms in view of Inventor's Disclosure:

"Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, b ut in the context of the entire patent, including the specification."

. . .

"For that reason, claims must be read in view of the specification, of which they are part . . . [T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term . . . "

"Consistent with that general principle, our cases recognize that the specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor's lexicography governs. . . . In other cases, the specification may reveal an intentional disclaimer, or disavowal, of claim scope by the inventor. In that instance as well, the inventor has dictated the correct claim scope, and the inventor's intention, as express in the specification, is regarded as dispositive." *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) (en banc).

Applicant respectfully requests entry of the amendment and allowance of Claims 1 - 21.

Respectfully,

/ Robert Frantz /

Robert H. Frantz, Reg. No. 42,553
Agent for Applicant
Tel: (405) 812-5613
Franklin Gray Patents, LLC